

PR1712939

JONES DAY

250 VESEY STREET • NEW YORK, NEW YORK 10281-1047
TELEPHONE: +1.212.326.3939 • FACSIMILE: +1.212.755.7306

PR1712939

June 20, 2017

Via First Class Mail and E-Mail

The Honorable George Jepsen
Attorney General
Office of the Attorney General
55 Elm Street
Hartford, CT 06106

Re: Recent Sabre Hospitality Solutions Data Breach

Dear Attorney General Jepsen:

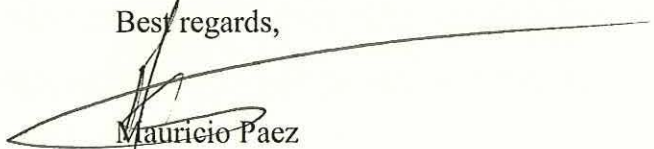
I am writing to give you advance notice of a data privacy breach affecting employees of our firm, Jones Day. This breach involves an estimated 3 individuals residing in your State.

On June 14, 2017, our travel services provider, Lawyers Travel Services, informed us that an unauthorized individual gained access to the travel reservation system of Sabre Hospitality Solutions ("Sabre"), a third party vendor for Lawyers Travel Services, between August 10, 2016 and March 9, 2017. Unfortunately, Sabre believes the unauthorized individual may have obtained access to certain personal information, including some of our employees' names, addresses, credit or debit card numbers, and possibly payment card security access codes.

Jones Day will notify the identified individuals this week. An exemplar copy of the notice letter is enclosed for your information. As the enclosed letter from Sabre explains, Sabre has taken steps to protect the security of its systems. We will be providing a full package of credit protection services and credit insurance for one year free of charge to the affected individuals.

Should any significant new information arise, we will promptly inform you. In the meantime, please do not hesitate to contact me if I can provide you with any additional information.

Best regards,


Mauricio Paez

(212) 326-7889

mpaez@jonesday.com

Enclosure

ALKHOBAR • AMSTERDAM • ATLANTA • BEIJING • BOSTON • BRISBANE • BRUSSELS • CHICAGO • CLEVELAND • COLUMBUS • DALLAS
DETROIT • DUBAI • DÜSSELDORF • FRANKFURT • HONG KONG • HOUSTON • IRVINE • JEDDAH • LONDON • LOS ANGELES
MADRID • MEXICO CITY • MIAMI • MILAN • MOSCOW • MUNICH • NEW YORK • PARIS • PERTH • PITTSBURGH • RIYADH
SAN DIEGO • SAN FRANCISCO • SÃO PAULO • SHANGHAI • SILICON VALLEY • SINGAPORE • SYDNEY • TAIPEI • TOKYO • WASHINGTON



SABRE HOSPITALITY SOLUTIONS

NOTICE OF DATA BREACH

Dear Valued Customer:

We are writing to you because of an incident involving unauthorized access to customer information associated with your hotel reservation(s). The privacy and protection of our customers' information is a matter we take very seriously, and we recommend that you closely review the information provided in this letter for some steps that you may take to protect yourself against potential misuse of your information.

What Happened?

The Sabre Hospitality Solutions SynXis Central Reservations system (Hospitality CRS) facilitates the booking of hotel reservations made by consumers through hotels, online travel agencies, and similar booking services. Following an examination of forensic evidence, Sabre notified us on or about June 6, 2017 that an unauthorized party gained access to account credentials that permitted unauthorized access to unencrypted payment card information, as well as certain reservation information, for a subset of hotel reservations processed through the Hospitality CRS.

The investigation determined that the unauthorized party first obtained access to payment card and other reservation information on August 10, 2016. The last access to payment card information was on March 9, 2017.

What Information Was Involved?

The unauthorized party was able to access payment card information for your hotel reservation(s), including cardholder name; card number; card expiration date; and, potentially, your card security code. The unauthorized party was also able, in some cases, to access certain information such as guest name, email, phone number, address, and other information. Information such as Social Security, passport, or driver's license number was not accessed.

What We Are Doing

Sabre engaged a leading cybersecurity firm to support its investigation. Sabre also notified law enforcement and the payment card brands about this incident.

What You Can Do

You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported.

In addition, you may contact the Federal Trade Commission (FTC) or law enforcement, such as your state attorney general, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission 600
Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
<https://www.identitytheft.gov/>

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide credit reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the credit reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at <https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf>, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major credit reporting agencies to request a copy of your credit report.

Place a Fraud Alert or Security Freeze on Your Credit Report File

In addition, you may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last 90 days. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. The credit reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. You may be charged to place or lift a security freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

You may contact the nationwide credit reporting agencies at:

Equifax
P.O. Box 105788
Atlanta, GA 30348
(800) 525-6285
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(800) 680-7289
www.transunion.com

Please see the following page for certain state-specific information.

For More Information

We apologize for any inconvenience caused by this incident. If you have any questions regarding this incident or if you desire further information or assistance, please do not hesitate to contact us at [TELEPHONE NUMBER (toll-free, if available) OF PERSON OR BUSINESS REPORTING THE BREACH].

Sincerely,

[SIGNATURE]

RECEIVED
JAN 10 2010
FBI - NEW YORK
JAN 10 2010

IF YOU ARE A MARYLAND RESIDENT:

You may obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

RECEIVED
2017 JUN 27 PM 12:34
ATTORNEY GENERAL
ADMINISTRATION